Magdalena Garlikowska
Dr
Jednostka Inspekcyjna INFRACERT TSI

DOI: 10.35117/A_ENG_21_05_03

The formal and legal process of conducting an independent risk management assessment in rail transport

Abstract: Striving to increase the safety of rail transport is a priority for the European Union and all rail entities. One of the areas of this safety is risk management in connection with changes introduced to the railway system. Every entity operating on the railway market is obliged to do so. The article discusses the risk management process carried out by the Applicant - from the assessment of the significance of the change, through the risk analysis, to the submission of documents to the inspection (assessment) unit for independent assessment of the correctness of the risk management carried out by the Applicant.

Keywords: Independent assessment; Security; Risk assessment; Risk management

Introduction

The safety of rail transport is a priority for all entities operating on the rail market. The European Union has been ensuring rail interoperability for many years, as evidenced by, inter alia, issuing appropriate legal regulations containing requirements for these entities. Their purpose is to adapt national rules in such a way that the safety level of the European rail system is ensured and maintained.

The issues related to risk assessment in rail transport have gained importance in recent years. The source of this state of affairs is the EU regulations obliging the Member States to carry out the valuation and risk assessment in order to increase the safety level of the railway system. The railway system is still developing, and the numerous changes introduced to it in all areas are subject to the necessity to evaluate them in terms of their importance.

In Poland, intensive modernization of the railway network is underway, the rolling stock and railway equipment are modernized, and elements of the railway track are replaced. Therefore, technical projects and extensive documentation are created. Contractors, investors, and principals should assess the risk at different stages of the project, in all possible areas, having a choice of methods and techniques. This is expected to reduce the risk of errors that can lead to undesirable, sometimes catastrophic, outcomes.

Safety of the railway system

The safety of rail transport has been discussed for a long time, but it was only the Railway Safety Directive [2] that formalized the provisions in this area, obliging all Member States to maintain an appropriate level of this safety and, if possible, to constantly improve it. Along with the directive, such concepts as: security management, risk management, risk analysis appeared. A systemic approach to the discussed issue was introduced. It turned out to be necessary, among others due to more and more new, extremely complex technologies, an increase in train speed, a large number of railway carriers. Aspects related to traffic management and safety systems required a risk analysis, both own and resulting from joint operations, and the transfer of threats between independent entities of the railway industry - infrastructure managers and carriers.

The requirements in this respect were maintained and clearly defined by Directive 2016/798 in the matter of safety [3], obliging railway operators to adopt a systemic approach in the area of safety and cooperation in order to ensure it and continuously improve it.
The following steps were found to be necessary to ensure the safety:

- harmonization of the regulatory structure,
- defining the responsibilities of the subjects in the railway system,
- development of common safety requirements (CST - Common Safety Target) and common safety methods (CSM - Common Safety Methods) enabling the harmonization of regulations at the EU level,
- establishing the rules for issuing, extending, changing, and limiting or withdrawing safety certificates and safety authorizations,
- the requirement to establish for each Member State a national safety authority (UTK in Poland) and an investigative body (accidents and incidents),
- defining common rules for safety management and supervision.

The following entities play a role in the development and improvement of railway safety:

1. Countries
2. European Union Railway Agency
3. Infrastructure managers and railway carriers:
    - implement the necessary risk control measures, also in cooperation with each other and with other actors,
    - implement safety management systems and take into account the risks associated with the activities of other entities and third parties,
    - in justified cases, they oblige other entities having a potential impact on the security of the system to implement the necessary risk control measures,
    - ensure that their contractors apply risk management measures by using the CSM to monitor the processes defined in the CSM.

Entities responsible for the maintenance of infrastructure and rolling stock.
The areas of risk analysis in the context of changes introduced to the railway system are the following subsystems:

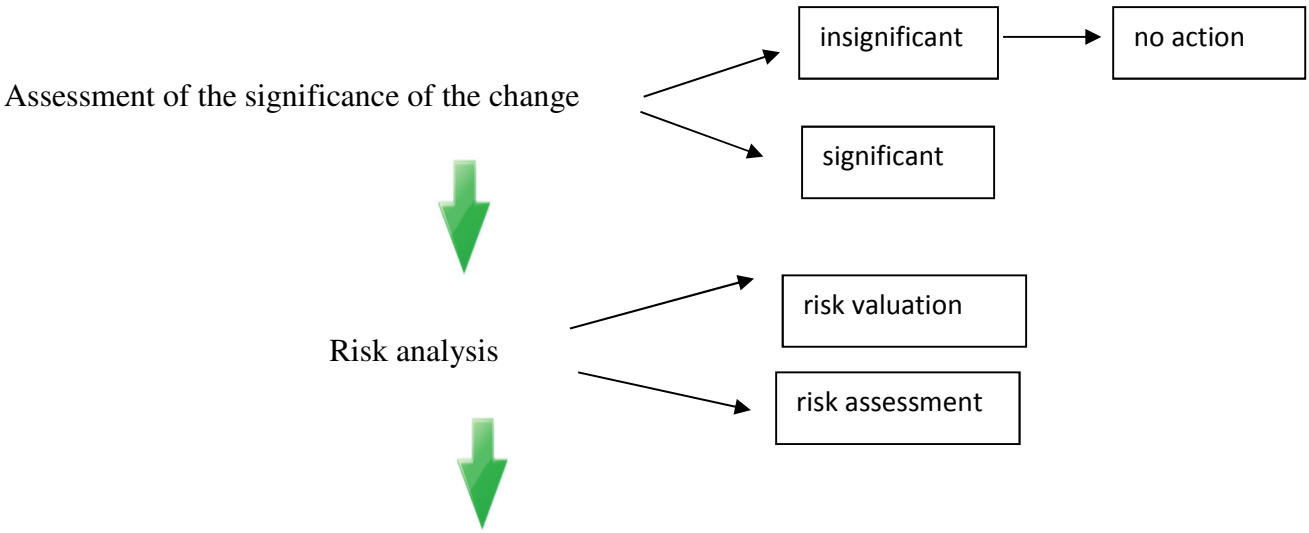
a) structural
    - Infrastructure subsystem, including Infrastruktura-PRM
    - Energy subsystem
    - The control-command subsystem
    - Tabor subsystem.
b) functional
    - Railway traffic subsystem
    - The Maintenance subsystem
    - Telematics Applications subsystem.

Until recently, changes could also be assessed in the management systems: QMS, SMS, and MMS, however, as a result of the agreement between the EU Railway Agency (ERA) and the accreditation bodies, inspection bodies have abandoned this scope.

The process of risk assessment

The basis for the risk evaluation and assessment process is Regulation No. 402/2013 on a common safety method for risk evaluation and assessment [7] and Regulation No. 1136/2015 amending the above-mentioned regulation [8].

The process can be divided into 3 general steps as shown in the diagram **1** below:



1. Risk assessment diagram, source: own elaboration

Stage I - Assessment of the significance of the change

The risk analysis process begins with the definition of change and its potential impact on the safety of the railway system. Each change introduced to the railway system is assessed in terms of its significance. If a change is classified as insignificant, i.e. having no impact on safety, there is no need to apply the risk management process. If the proposed change has an impact on safety, the evaluating entity shall, based on professional judgment, decide on the significance of the change taking into account the 6 criteria described in Article 4 of Regulation No. 402/2013, i.e.:

- system crash effects (worst case scenario),
- innovation used in introducing the change (in the organization and/or the entire railway sector),
- complexity of change,
- monitoring (the ability to monitor changes throughout the entire life cycle of the system and to make appropriate interventions),
- reversibility of the change (possibility of returning to the system from before the change),
- additionality (inclusion in the assessment of all recent safety-related changes to the assessed system that were classified as insignificant),

It is assumed that in the event of any of the above-mentioned the criterion qualifies the change as significant, although there are no indications in this respect in the legal regulations. Then it is necessary to conduct a risk analysis. If the assessment team considers the change to be insignificant - there is no such requirement, which is not a good solution as it makes it impossible to obtain a lot of important information, such as:

- identifying new threats,
- checking what risk they are related to,
- definition of risk management measures,
- risk mitigation possible [4].

Stage II - Risk analysis

After the change is classified as significant and having an impact on the safety of the railway system, an interdisciplinary team appointed for this purpose begins to analyze the risk that the introduced change may entail.

The team analyzes and documents the following:

1. System definition - its purpose, functions, boundaries, interfaces, environment, existing security measures, security requirements;
2. Identification and classification of threats - determination of all rationally foreseeable threats, systematization of them according to the estimated risk for them, an indication of generally acceptable threats for which the risk is negligible, i.e. no further analysis is required;
3. Risk acceptability testing - selection of the risk acceptance method (principle) - codes of conduct, comparison with similar systems, estimation of explicit risk;
4. Risk valuation - an element of the analysis performed with the use of the selected risk acceptance principle (or principles), leading to determining whether the risk, after applying a given principle, is within the admissibility limits;
5. Indication of safety requirements and demonstration of compliance with safety requirements - ensuring that the system is designed, constructed, and put into operation based on the specified safety measures;
6. Transfer of documentation to an inspection body for independent assessment.

Stage III - Independent assessment by the inspection body

The risk analysis performed by the team along with the assessment of the significance of the change is forwarded to the inspection unit for independent safety assessment. The inspection body operates within the scope of its accreditation in accordance with the standard 17020: 2012 [5] and the document DAK-08 [1], issued by the Polish Center for Accreditation. The unit verifies the correctness of the risk evaluation and assessment process by checking:

- completeness of the description of the system subject to change,
- completeness of identification of all reasonably foreseeable threats to the system and their classification,
- if all hazards and related safety and risk control measures in the hazard log are included,
- indication in the risk register of persons or positions responsible for the application of security measures or risk control aimed at reducing the associated risk
- with the threats specified in the subject of the change,
- identification by the Applicant of all interfaces relevant to the assessed railway system and the correctness of the risk management process at the interfaces,
- security requirements that the system should meet,
- information on risk monitoring related to identified hazards,
- correctness of use of a given method to identify hazards,
- correctness of the application of a given risk acceptance principle for the assessed change and its compliance with the minimum requirements resulting from Regulation No. 402/2013,,
- demonstrating compliance with safety requirements,
- ensuring safe integration of the proposed change into the system as a whole,
- documenting the risk management process in a complete manner and enabling its verification by the assessment unit..

As a result of the assessment of the above-mentioned components by the inspection body is a safety assessment report. The form of drawing up the report complies with the procedures of a given inspection unit.

Safe integration

From January 2020, pursuant to additional regulations issued by the EU Railway Agency, inspection bodies are required to assess the safe integration of the change into the system. It is therefore logical that entities introducing changes to the system must address this issue in their risk analysis report.

It turns out that entities in the railway sector have different understandings of the concept of safe integration. It is often understood only as a demonstration of technical compliance and the existence of valid technical interfaces between subsystems, but this is not the correct understanding. It can be said that safe integration is an integral part of the risk assessment and risk management process, which means that it has a broader meaning than just a one-time technical compliance check or identification of interfaces. It is valid at various levels and covers the entire life cycle of the design, operation, maintenance, and decommissioning of the railway system and its components [6].

Whenever a new element is introduced into the railway system or an existing one is modified, irrespective of the significance of the change, the railway entity has to integrate safely and carry out a risk assessment and risk management. It is imperative to ensure that:

- the new or modified element is technically compatible with other parts of the system into which it is introduced,
- the new or modified element has been designed to be safe and meets all the assumed functional and technical purposes,
- the impact of the human factor and organizational aspects on the operation and maintenance of this element and the system has been assessed and taken into account,
- the introduction of a new or modified element will not bring about unfavorable and unacceptable effects on the safety of the system after switching on this element.

The architecture of the railway system is complicated, so the safe operation of a given system depends to a large extent on the safety of the technical subsystems constituting it, as well as the safe organization and correct division of roles and responsibilities among the interested railway entities. Therefore, safe integration of change depends on the correct understanding of the broadly understood context of this change (physical, functional, environmental, operational), all interrelationships and the relationship between the change and the rest of the railway system, the roles, and responsibilities of each party involved in the area related to the change. It should be kept in mind that the responsibility in this area does not only rest with a single railway entity, but also with every other railway network operator and operator. These subjects, therefore, share this responsibility - each for their own part of the system. This fact has to be taken into account in the risk analysis, in particular in the hazard register.

Inspection body experience

The need to assess the significance of the change and conduct a risk analysis generates many problems for both assessment teams and inspection bodies.

The first such problem is the lack of indications in the legal regulations on how to apply the criteria for assessing the significance of the change contained in Regulation No. 402/2013. Only one criterion must be met whether all these criteria have to be met, or whether a change is considered significant. Only professional judgment counts here, which generates the need to create interdisciplinary assessment teams.

The second problem is the approach to the advisability of conducting risk analysis. If a change is classified as insignificant, i.e. having no impact on safety, there is no need to apply the risk management process, and therefore, as already mentioned, it is not possible to obtain a lot of relevant information on possible threats and their control measures. Such an approach may be due to a lack of understanding of the purpose and the possibility of using the effects of the risk analysis process. Instead of perceiving risk analysis as a possible source of information necessary for safety management, including project management, it is treated by employees as an unnecessary addition that hinders work.

The third problem relates to the identification of threats. Often there is an excessive aggregation of threats or their excessive fragmentation. It is forgotten to update the threat registry on an ongoing basis. It usually does not annotate the progress of risk monitoring. With shared risk, there is no clear distinction between threats. The concept of "substantially acceptable risk" is sometimes incomprehensible to those carrying out the risk analysis, which results in its uncritical assignment to threats.

Another area that generates errors in risk analysis is the application of risk acceptance principles and risk management measures. They are used incorrectly or inadequately,
for example, reference is made to outdated codes of conduct or documents that are not codes of conduct and is compared with an inadequate reference system. The effects of a system failure are given a low (usually underestimated) weight when estimating explicit risk. There are also no explicit statements on the acceptability of the risk.

The last observed problem is verification by an inspection body. It is worth concluding a contract with such an entity at the earliest possible stage. It is important both for technical and substantive reasons - the research period is shortened, there is a better understanding of the change and the entire process of risk evaluation and assessment. Often, applicants miss the fact that inspection bodies have a different scope of accreditation. This means that they can only perform the assessment to the extent to which they are accredited. There is also the financial issue - the evaluation unit is selected only in terms of the price of the service, and not e.g. its many years of experience on the market and its specialized employees.

It should be noted, however, that the awareness of Applicants is increasing and they report fewer problems than 2-3 years ago.

Summary

Risk management is obligatory for entities operating on the railway market, especially infrastructure managers and carriers. EU regulations require a risk analysis when introducing any change to the railway system. The significance of this change, judged on the basis of expert judgment, will determine whether a risk management process is implemented. A legal gap in this area has been noticed not only by national assessment units but also at the level of the European Union Railway Agency. The consequence of this is the currently most important postulate of qualifying changes as significant and not ignoring the need to implement the risk management process.

Risk assessment and risk management is the process of implementing a systemic approach. Its use can help to avoid many mistakes at different stages of the project, and thus increase the security of implemented investments. This is of particular importance in railway infrastructure investments, where the safety of passenger and freight transport is at stake.

The assessment of the impact of a change on railway safety should be performed at various levels - element/device, subsystem, the whole system, taking into account the responsibility of various interested parties. Failure to thoroughly analyze these changes will lead to a situation where some threats/risks to the railway system will remain unidentified, and therefore out of control.

Source materials

[1] DAK-08 *Akredytacja jednostek inspekcyjnych w obszarze działań objętych Rozporządzeniem Wykonawczym Komisji (UE) nr 402/2013*.
[2] Dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 roku w sprawie bezpieczeństwa kolei wspólnotowych.
[3] Dyrektywa 2016/798 Parlamentu Europejskiego I Rady (UE) z dnia 11 maja 2016 r. w sprawie bezpieczeństwa kolei.
[4] Garlikowska M., Gondek P., *Bezpieczeństwo i ryzyko w systemie kolejowym Unii Europejskiej,* Prace Instytutu Kolejnictwa, Zeszyt nr 157, Warszawa 2018.
[5] Norma 17020:2012 *Ocena zgodności. Wymagania dotyczące działania różnych rodzajów jednostek przeprowadzających inspekcję.*
[6] Nota objaśniająca w sprawie bezpiecznej integracji, ERA 1209/063 wersja 1.0.
[7] Rozporządzenie nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka.
[8] Rozporządzenie nr 1136/2015 z dnia 13 lipca 2015 r. zmieniające rozporządzenie wykonawcze (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka.